



To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

REVISION: This revised directive supersedes TSA MD 1000.7, U.S. Debit Card, dated July 20, 2015.

SUMMARY OF CHANGES: Section 5, Responsibilities, changed from Financial Management Division to Office of Finance and Administration's Financial Management Division; added minor edits for clarification throughout the directive.

1. **PURPOSE:** This directive provides TSA policy and procedures governing the use of the United States (U.S.) debit card.
2. **SCOPE:** This directive applies to all TSA organizational elements and employees.
3. **AUTHORITIES:**
 - A. 31 USC § 3302, Custodians of Money
 - B. Department of the Treasury Financial Manual (TFM) Volume I, Part 4A, 3000, Requirements for Scheduling Payments Disbursed by the Bureau of Fiscal Service (Fiscal Service)
 - C. Government Charge Card Abuse Prevention Act of 2012
 - D. Office of Management and Budget Circular A-123, Management's Responsibility for Internal Control, Appendix B, Improving the Management of Government Charge Card Programs
 - E. [TSA MD 1100.75-3, Addressing Unacceptable Performance and Conduct](#)

4. DEFINITIONS:

- A. **Abuse:** Use of a Government charge or debit card to buy authorized items, but at terms (e.g., price, quantity) that are excessive, that are not for a *bona fide* Government need, or both.

Example: The purchase of items such as a day planner costing \$300 rather than \$45, awards-ceremony refreshments exceeding TSA's policy cost ceiling of \$5 per attendee, or year-end or bulk purchases of computer and electronic equipment without a *bona fide* government need.

- B. **Automated Standard Application for Payments (ASAP):** A secure, web-based, all-electronic payment and information application that allows federal agencies to choose

TSA MANAGEMENT DIRECTIVE No. 1000.7
U.S. DEBIT CARD

from three payment models to fit their financial needs and streamline operations at no charge to the federal agencies or their payment recipients.

- C. Component Primary Organization Program Coordinator (CPOPC): An individual designated by the Chief Financial Officer (CFO) to administer and monitor the contractor-issued debit cards for TSA.
- D. Fraud: For the purpose of this directive, the use of a Government charge or debit card for any unauthorized purpose or for any purpose other than official government business.
- E. Government Charge Card: A magnetic-stripe payment card that draws from an account established through a commercial financial institution (hereinafter, "charge card vendor") on behalf of agencies or individual agency employees to which the cost of purchasing goods and services may be charged.
- F. Misuse: Use of a Federal charge or debit card for other than the official Government purpose(s) for which it is intended and authorized.
- G. Organization Program Coordinator (OPC): An individual designated within each TSA program area or office responsible for oversight of the contractor-issued debit card activity within his/her respective area.
- H. Pecuniary Liability: The obligation of a charge or debit card user to personally repay losses resulting from illegal, improper, or incorrect payments or uses of the charge or debit card or the funds received through their use. This obligation to personally repay losses includes the physical loss of cash and inability to properly account for cash expenditures.
- I. Program/Field Office: An organizational unit within TSA authorized to commit and/or obligate funds on TSA's behalf (e.g., airport offices and Financial Management Division), within the limits of TSA's Budget Execution and Acquisition policies.
- J. U. S. Debit Card (Debit Card): A magnetic-stripe payment card that provides the cardholder electronic access to stored monetary value.

5. RESPONSIBILITIES:

- A. The Office of Finance and Administration's Financial Management Division (FMD) is responsible for:
 - (1) Establishing internal control procedures and performance metrics to monitor misuse, spending, and other transaction activities for identification of fraud, waste, and abuse of the debit card;
 - (2) Designating a Component Primary Organization Program Coordinator (CPOPC) and Agency Program Coordinator (APC), who will serve as an administrator of the debit card program and act as a liaison between TSA, Fiscal Service and the debit card program contractor on program issues;

TSA MANAGEMENT DIRECTIVE No. 1000.7
U.S. DEBIT CARD

- (3) Reviewing debit card applications for accuracy and, as appropriate, approving and forwarding the debit card applications to the debit card contractor for further processing;
- (4) Ensuring APCs, OPCs and users review TSA MD 1000.7 and submit a signed copy of [TSA Form 1007, Debit Card Request and Agreement](#), acknowledging agreement to the terms to finance@tsa.dhs.gov mailbox prior to issuing a debit card to the requesting office;
- (5) Ensuring the activities of the program and field offices are in compliance with the Debit Card Program;
- (6) Maintaining and updating debit card accounts within their respective area;
- (7) Administering and monitoring all debit card transactions within their purview for appropriate use;
- (8) Promoting correct and efficient use of the debit card;
- (9) Ensuring oversight of appropriate corrective action for misuse of the debit card;
- (10) Referring potential cases of fraud, waste, and abuse, as appropriate, to the TSA Office of Inspection (OOI) or DHS Office of Inspector General (OIG); and
- (11) Adhering to Privacy Act requirements at all times.

B. Debit Card APCs are responsible for:

- (1) Ensuring OPCs and users review TSA MD 1000.7 and submit a signed copy of [TSA Form 1007](#) acknowledging agreement to the terms to finance@tsa.dhs.gov mailbox prior to issuing a debit card to the requesting office;
- (2) Reviewing limits and approving user requests to fund individual debit cards, as appropriate, when emergency mission-critical circumstances arise;
- (3) Reconciling posted debit card transactions with receipts received by the program or field offices to transactions posted in the contractor's debit card system;
- (4) Serving as the liaison between TSA, Fiscal Service, and the debit card program contractor on issues with the program;
- (5) Assisting OPCs, as necessary, in managing the debit card programs in their respective areas. Assistance may include, but is not limited to, providing OPCs access to necessary tools and reports, issuing new debit cards when current cards are expiring, canceling lost or stolen debit cards, and providing guidance on the disposition of cash and debit cards;

TSA MANAGEMENT DIRECTIVE No. 1000.7
U.S. DEBIT CARD

- (6) Referring potential cases of fraud, waste, and abuse, as appropriate, to TSA OOI or DHS OIG; and
- (7) Adhering to Privacy Act requirements at all times.

C. Program Offices Directors and Federal Security Directors (FSDs) are responsible for:

- (1) Designating an OPC responsible for oversight of the debit card program within his or her program or office;
- (2) Ensuring OPC and users review TSA MD 1000.7 and submit a signed copy of [TSA Form 1007](#) acknowledging agreement to the terms to finance@tsa.dhs.gov mailbox prior to processing an application, as well as including a copy of the completed form in each request for funding when an anticipated emergency arises;
- (3) Implementing and enforcing debit card policies and procedures;
- (4) Requiring OPCs and supervisors to ensure that any card misuse is addressed and corrective action is taken to prevent further occurrences of misuse;
- (5) Retrieving the debit card from an employee user when the employee leaves TSA or transfers to a TSA position that does not require a debit card or to a different program/field office;
- (6) Referring potential cases of fraud, waste, or misuse to his or her CPOPC, TSA OOI or DHS OIG; and
- (7) Adhering to Privacy Act requirements at all times.

D. Debit Card OPCs are responsible for:

- (1) Implementing TSA debit card policies and procedures;
- (2) Instructing the user that the debit card(s) and all cash acquired using it (e.g., cash withdrawn at a financial institution or an ATM) should be kept in a secure location;
- (3) Reviewing TSA MD 1000.7 and submitting a signed copy of [TSA Form 1007](#) acknowledging agreement to the terms to finance@tsa.dhs.gov mailbox upon requesting a debit card;
- (4) In the event a debit card is lost or stolen, immediately contacting the CPOPC to have the card closed and replaced;
- (5) Ensuring receipts are kept in a secure location and are provided to the CPOPC upon request;
- (6) Performing monthly reviews of transaction reports to ensure appropriate use of Federal funds disbursed through the debit card program;

TSA MANAGEMENT DIRECTIVE No. 1000.7
U.S. DEBIT CARD

- (7) Notifying the Bank immediately of any lost, stolen, or damaged debit cards;
- (8) Performing monthly reviews of transaction reports and other bank-generated reports to ensure appropriate use of Federal funds disbursed through the debit card program;

NOTE: Results of the reviews must be provided to the APC by the 25th of each month (if the 25th falls on a Saturday, then it is due on the previous Friday; if it falls on a Sunday, then it is due on the following Monday);

- (9) Notifying the bank of any billing discrepancies (e.g., disputes) regarding charges posted to an account by completing the dispute form on the [Metabank's website](#) within the required timeframe;
 - (10) Returning unused funds back to the appropriation from which they came;
 - (11) Suspending a multiple-use card if there is a pattern of inappropriate use;
- NOTE:** Refer all instances to the OIG and institute appropriate disciplinary action;
- (12) Conducting reviews of the Debit Card Program at least annually;
 - (13) Referring potential cases of fraud and abuse, as appropriate, to the CPOPC, TSA OOI or DHS OIG; and
 - (14) Adhering to Privacy Act requirements at all times.

E. Debit Card Users are responsible for:

- (1) Reviewing TSA MD 1000.7 and submitting a signed copy of [TSA Form 1007](#) acknowledging agreement to the terms to finance@tsa.dhs.gov mailbox upon requesting a debit card;
- (2) The cash value of the card. Loss of funds through misuse of the debit card or through the failure to properly safeguard it and its Personal Identification Number (PIN) may result in personal liability for the lost funds;
- (3) Using the debit card, including cash obtained with it, only for specific official TSA business or authorized purposes for which it was issued. Use of the debit card does not relieve employees of their responsibility to employ prudent practices when incurring Government expenses;
- (4) Complying with this directive and with the program or field office's internal procedures;
- (5) Complying with Office of Contracting and Procurement procedures. The debit card may not be used in place of a TSA Purchase Card;

NOTE: In the event of an emergency in which conditions such as power outages prevent the use of a Purchase Card, cash obtained with the debit card may be used to make urgent purchases of emergency supplies (See section 6.A (.3)). Cash withdrawn can be used only for emergency-related purchases. Purchases made directly with the debit card in anticipation of an emergency are prohibited.

- (6) Ensuring that charges and/or cash withdrawals placed against the debit card account do not exceed its value. Generally, electronic controls at ATMs and financial institutions will prevent the card from being overdrawn. However, limitations of the electronic banking system may result in accounts being overdrawn, and the user may be personally liable for such overdrafts;
- (7) Submitting all transaction receipts or invoices, regardless of the amount, to the OPC or his or her designee and maintaining copies;
- (8) Keeping accurate, up-to-date records of all debit card usage, and retaining all receipts;
- (9) Notifying the applicable OPC and/or the CPOPC immediately if additional card funding is anticipated before attempting to withdraw the additional funds. Withdrawal above any authorized amount not approved in advance will constitute misuse of the debit card and will subject the user to disciplinary action;
- (10) Safeguarding the debit card and its PIN, and ensuring the card and all cash acquired using the card is held in a secure location;
- (11) Immediately advising the OPC and/or the CPOPC to close the debit card account if the card is lost or stolen; and
- (12) Returning any unused funds to TSA Headquarters (HQ) or depositing the funds in the appropriate financial institution, as directed by the CPOPC, as soon as the need to hold the funds no longer exists.

6. POLICY:

A. Use of the Debit Card:

- (1) Program and field offices will be issued a debit card for use only in mission-specific situations requiring cash or in emergency situations, when the standard acquisition procedures (either the Purchase Card or the procurement contracting process) cannot be used. Debit cards are assigned to the organization, not to an individual.
- (2) Under the direction and approval of the FMD Director, the program or field office will establish written policies governing the use and control of imprest funds, local accounts at a depository institution, and secure on-site storage of funds. The program or field office also will implement other management controls as may be required or prudent under the circumstances.

- (3) The Debit Card may be loaded with a specified amount and reloaded as necessary to make multiple payments. The Debit Card may be used only in limited mission-specific circumstances to make miscellaneous or nonrecurring payments, or to allow Government employees access to cash in performance of their official duties. Fiscal Service administers the Debit Card program.

NOTE: The Debit Card is distinct from the travel card, purchase card, and fleet card.

- (4) If a debit card is used for any purpose other than as stated in 6.A.(1), the Program Office must request an advance waiver from FMD leadership.

B. Misuse of the Debit Card:

- (1) Use of the debit card for any expense or withdrawal of funds other than for the official business or authorized purposes for which it was issued shall be considered misuse of the debit card.
- (2) Use of debit card to pay for personal expenses shall be considered misuse of the debit card.
- (3) All TSA employees (including, without limitation, financial management personnel) must report fraud, waste, or abuse to their supervisor or the OOI hotline at 571-227-1800 or TSAInspectionHotline@dhs.gov.
- (4) Misuse of the debit card may result in disciplinary action. Any disciplinary action must be consistent with the provisions outlined in [TSA MD 1100.75-3, Addressing Unacceptable Performance and Conduct](#). Disciplinary actions must be coordinated with designated HQ or field counsel and OHC HQ Employee Relations staff.
- (5) Debit card users will be accountable and may be held personally liable for any unauthorized or unofficial purchases or cash receipts.

7. PROCEDURES:

- A. To obtain a debit card, contact the FMD Accounting Branch (AB) Point of Contact at finance@tsa.dhs.gov.

- (1) Debit cards will not be issued without a signed copy of [TSA Form 1007](#).
- (2) The amount usually placed on the card is between \$500 and \$1,000 for emergency funds. These funds are for emergency use only and will be placed on the card only upon approval by the FMD Director, FMD Deputy Director, or FMD AB Chief.

- B. Send any request for funds to be placed on a debit card for potential cash withdrawal to the FMD AB Chief, with a copy to the airport FSD, if applicable, via finance@tsa.dhs.gov. The request must state the amount of the withdrawal, justification for the withdrawal, and approval by an authorized official at the program level. Include a copy of the signed [TSA Form 1007](#) in the email request.

TSA MANAGEMENT DIRECTIVE No. 1000.7
U.S. DEBIT CARD

C. Safeguard the debit card and its PIN by ensuring the card and all cash acquired using it (e.g., cash withdrawn at a financial institution or an ATM) are held in a secure location. Return unused funds to TSA HQ or deposit the funds in the appropriate financial institution, as directed by the CPOPC, and as soon as the need to use the funds dissipates. Debit cards that are not needed should be either returned to HQ or destroyed, as directed by the CPOPC.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date it is signed unless otherwise specified.

APPROVAL

Signed

August 1, 2017

Pat A. Rose, Jr
Assistant Administrator/
Chief Financial and Administrative Officer

Date

EFFECTIVE

Date

Distribution: Assistant Administrators and equivalents, Managers and Supervisors, Business Management Division Directors and MD POCs

Point-of-Contact: FMD Financial Policy and Travel Branch
TSAFinancialPolicy@tsa.dhs.gov